PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 9/00 — A1

(11) International Publication Number: WO 00/65765

(43) International Publication Date: 2 November 2000 (02.11.00)

(21) International Application Number: PCT/FI00/00353

(22) International Filing Date: 25 April 2000 (25.04.00)

(30) Priority Data:
990936 26 April 1999 (26.04.99) FI

(71) Applicant *(for all designated States except US)*: NOKIA NETWORKS OY [FI/FI]; P.O. Box 300, FIN-00045 Nokia Group (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: HAUMONT, Serge [FR/FI]; Riistavuorenkuja 3 B 10, FIN-00320 Helsinki (FI).

(74) Agent: BERGGREN OY AB; P.O Box 16, FIN-00101 Helsinki (FI)

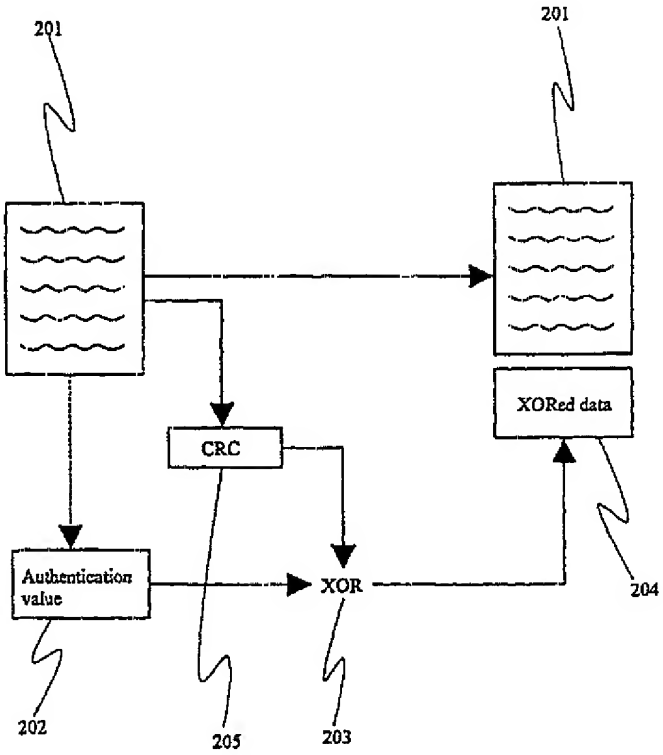
(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG)

Published
With international search report
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments

(54) Title: NEW METHOD FOR CHECKING THE DATA

(57) Abstract

This invention concerns the checking of data in a systems where the security is an important issue. According to the invention a first reference value is calculated at least partly based on a first error check value calculated from the data and a first authentication value (202). When checking the data a second error check value is calculated from the data. As well, a second reference value is calculated at least partly based on a first and a second value from the set of the second error check value, a second authentication value and the first reference value. The second reference value is compared with a third value from the set of the second error check value, the second authentication value and the first reference value. The invention also comprises a transmitter and a receiver which are arranged to perform the described operations.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People s Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

New method for checking the data

The invention concerns the security of the data transmission and the checking the data, especially in digital mobile telecommunication networks.

Security is becoming more and more important in the field of communications. The paper-based communication is used less and modern electronic systems are used more and more. This trend increases the risk that information transmitted via electronic networks falls into the hands of somebody to whom it was not meant to. The data can also change during the transmission because of the different kinds of interference in the transmission path.

Methods have been developed by means of which the receiver can notice, if somebody has altered the data between the sending end and the receiving end. The same methods can be used to detect, if the data has changed as a result of interference in the transmission path. Usually these methods utilize some kind of error detecting algorithm codes, like parity checking.

One very effective method to carry out the error detection is to use the so called cyclic redundancy check (CRC). CRC is a very powerful but easily implemented technique for obtaining data reliability. The basic idea in CRC is that the transmitter appends an extra n-bit sequence to every data frame. This extra n-bit sequence is called frame check sequence (FCS). The FCS is generated by the transmitter from the original data frame. The resulting frame (the cascade of the original frame and the FCS) is divisible by some pre-defined polynomial which is called the CRC polynomial. In the receiving end the transmitted data frame is divided by the CRC polynomial. The remainder of the division is checked and if it equals to zero the transmitted data has not changed in the transmission path.

In addition to the error check there is need for securing the data so that nobody else than justified receiver is able to find out the content of the data frame. In principle there are two different security methods available. These methods are based on an algorithm or algorithms which are used to encrypt and decrypt the data. The first security method is based on a secret key method. In the secret key method there is used only one key or one algorithm to encrypt and decrypt the data. Both the sender and the receiver of the data use the same secret key. The most important point in the secret key method is that the key should be kept secret so that the only persons who know the key are the sender and the receiver. One of the biggest problems in the

secret key method is that the key should be transmitted secretively from the first user to another and this means that a third party has an opportunity to get the secret key.

The second security method is based on a so called secret and public key pair. A user creates these two keys. The public key is given available for everybody. All other users encrypt their messages meant for the publisher of the public key by using the public key. The encrypted message can be decrypted only with the secret key which is known only by the publisher of the keys. The advantage of the public key method is that there is no need to transmit the secret key and because of this the security is better than in the previously described secret key method. The power of the public and secret key method is that the method is mathematically very heavy so that the decryption of the encrypted data without the secret key takes so long time that the encrypted data is out-of-date when the decryption is accomplished without the correct keys.

Digital signature is used to identify the signer, who is the sender of the data. Advantageously in the digital signature method it is used the secret and public key method to achieve the signature for a certain data. Digital signature works for example like this: The sender of the message derives for example an error check value from the original message. After this the sender of the message encrypts the error check value with his secret key and sends the original message and the encrypted error check value to the receiver. The receiver decrypts the encrypted error check value with the sender's public key, which the sender has delivered to everybody. The receiver also derives the error check value from the original message and compares these two error check values. If the values are equal, the message is from the correct sender. If they don't equal, the message has been corrupted.

It is planned that the mobile telecommunication networks, like the GSM, will be capable to transmit the data as a data packets. In GSM this is achieved by combining a so called GPRS (General Packet Radio Service) network to the GSM network. In figure 1 it is shown one possible arrangement of the GPRS network. There is shown a mobile station 101, which is in connection to MSC (Mobile Switching Centre) 104 through BTS (Base Transceiver Station) 102 and BSC (Base Station Controller) 103. There can be attached different types of networks, like for instance PSTN (Public Switched Telephone Network) network 105 and SS7 network, to the MSC 104. A new network element is arranged to the BSC 103, which is called PCU (Packet Control Unit) 107. However, it is by no means compulsory that the PCU

(107) is located at the BSC (103), but it can be as a separate unit or attached to the BTS (102) as well. The PCU 107 is arranged to control the data packets. The packet network 112 is attached to other network topology through the PCU 107. Between the GPRS backbone network 113 and the PCU 107 it is arranged a SGSN (Serving GPRS Support Node) node 108. A GPRS register 109, or more generally a home location register that contains user related information, into which some kind of subscriber-related information concerning GPRS service network element is saved, is also a part of the GPRS network. GGSN (Gateway GPRS Support Node) nodes 110 are the elements through which any other kind of packet network 111, like IP, OSI data or X.25, can be attached to the GPRS network. In figure 1 the solid line symbolizes the data transmission and the signalling between the network elements and the broken line symbolizes that there are signalling between the network elements. A similar arrangement is planned to the third generation mobile telecommunication networks for transmitting the data as a packet data.

It is important to know that the received data is from the correct sender. The methods shown here are also applied to verify the sender of the data as previously shown. One possible way to do the verification is to derive a so called authentication value from the original data, which authentication value is a kind of digital signature. The authentication value can be arranged so that it may be derived from various inputs. The input can be e.g. a packet number, the direction (uplink or downlink) of the transferred packet, a secret key or any other similar value. The algorithm, by means of which the authentication value is calculated, is the same or the reverse at the sending end and at the receiving end. The algorithm is kept secret if it is not strong enough. The calculated authentication value is carried in each packet so that every single packet include the key by means of which the content of the data packet can be checked, whether is original or not. In the examples described in this application, usually the exclusive OR (XOR) mathematical function is used. However, it is evident to a man skilled in the art that any function f for which exists an inverse function f^{-1} so that $f^{-1}(f(x))$ gives x can be used as well.

This authentication method shown has one big disadvantage. It increases significantly the packet size, because the calculated authentication value is transmitted in every data packet separately from the rest of the data to be transmitted. As a result, a part of the capacity for data transmission is wasted because of these additional authentication value frames.

An object of the present invention is to provide a new method by means of which the authentication value can be transmitted in a packet data transmission network

without increasing the packet size. It provides a simple per packet authentication so that the receiver can with one check determine if the packet is valid or not. A second object of the present invention is to provide a transmitter, which is capable of arranging the authentication value into a packet so that the packet size is not increased. A third object of the present invention is to provide a receiver, which is capable of checking, if the transmitted data has changed in the transmission path. A fourth object of the present invention is to provide a mobile station which is capable of transmitting and receiving the authentication value without increasing the packet size

The above stated objects are achieved by combining the authentication value to the error check data so that it does not add the packet size. Combining the authentication value to error check data is done by using a logical function, for example At the receiving end the combination of the error check value and the authentication value is processed so that the integrity of the data can be checked

The advantage of the present invention is that by using this arrangement in a telecommunication system the bandwidth of the system can be saved. It also enables the use of digital signatures with fixed length frames of present protocols without changing the frame formats. As a result, the authenticity can be provided without increasing the packet size One very important aspect is that the invention is applicable in all digital communication systems.

The method according to the invention is characterized in that

- a first reference value is calculated using at least partly based on a first authentication value and a first error check value calculated from the data

The transmitter according to the invention is characterized in that the transmitter comprises

- means for deriving an authentication value (202) from the data to be transmitted (201),

- means for deriving an error check value from the data to be transmitted (201) and

- means for combining said authentication value (202) and said error check value with a logical function for producing a first reference value.

The receiver for receiving data having means for checking received data according to the invention is characterized in that the receiver comprises

- means for deriving a first reference value from the received data,

- means for calculating a second error check value from the received data,

- means for calculating a second reference value at least partly based on a first and a second value from the set of said second error check value, a second authentication value and said first reference value, and

- means for comparing said second reference value with a third value from the set of said second error check value, said second authentication value and said first reference value.

The station, comprising a transmitter and a receiver, according to the invention is characterized in that the transmitter comprises

- means for deriving an authentication value (202) from the data to be transmitted (201),

- means for deriving an error check value from the data to be transmitted (201) and

- means for combining said authentication value (202) and said error check value with a logical function for producing a first reference value

and

the receiver comprises

- means for deriving a first reference value from the received data,

- means for calculating a second error check value from the received data,

- means for calculating a second reference value at least partly based on a first and a second value from the set of said second error check value, a second authentication value and said first reference value, and

- means for comparing said second reference value with a third value from the set of said second error check value, said second authentication value and said first reference value.

The present invention will now be described more in detail in the following with the reference to the accompanying drawings, in which

fig. 1 illustrates one possible arrangement of the GPRS network,

fig 2 illustrates one possible arrangement at the sending end,

fig 3 illustrates one possible arrangement at the receiving end and

fig 4 illustrates a block diagram of a mobile station

In the present invention the data transmitted is processed at the both ends, that is at the sending end and at the receiving end, in the same way so that the integrity of the message can be checked. At the sending end, as shown in figure 2, the error check value, which in this preferred embodiment is a CRC 205, is derived from the original data 201. Next, the authentication value 202, which can be derived for instance by using a packet number or a secret key as an input and a secret algorithm, is combined to the CRC field. The broken line describes that the authentication value 202 is in some way derived from the original data 201. The combination of the CRC 205 and the authentication value 202 is carried out in this preferred embodiment of the invention by using the logical function "exclusive-OR" (XOR) 203. XOR 203 is a function which produces an output of 1 when exactly one of its two inputs is 1. As a result, the data, which is to be sent, comprises the original data field 201 and another field, which consists of the XORed value 308 of the CRC 205 and the authentication value 202. To a man skilled in the art it is obvious that the authentication value 202 can be any value, which is advantageously possible to derive from the original data 201.

At the receiving end the data received is arranged to be processed vice versa, as shown in figure 3. The XORed data 308 is re-XORed 203 with the authentication value 302, which is the same as the authentication value 202 at the sending end in a case where the data sent is not changed. The authentication value 302 can be derived from the received data 301 in the same way as at the sending end. By using the rules of binary algebra the result of this re-XORing 203 is CRC value 304. By comparing 305 this CRC 304 to another CRC 303 calculated at the receiving end from the received data, it can be found, if the data has changed in the transmission path. If the comparison 302 shows that the CRCs 303; 304 are the same, it means that the received data 301 has been transmitted without any changes 306. But, if the comparison 305 shows that the CRCs 303; 304 differ from each other, it means that the original data 201 has changed in the transmission path, or that the authentication value 302 was not correct at the receiving end. As a result, the data received can be erased 306.

To a man skilled in the art it is obvious that the method shown reveals all cases when the original data 201 has been processed between the sending end and the receiving end in condition that the algorithm for deriving the authentication value 202; 302 is kept secret. If the original data 201 has been changed, the CRCs 303; 304 differ from each other as previously stated. As well, if the authentication value 302 at the receiving end is not the same as the authentication value 202 at the sending end, the compared CRC values 303; 304 do not equal. The reason for this is that the XOR operation 203 to the XORed data 308 received and the authentication value 302 does not produce the original CRC value 205.

To a man skilled in the art it is obvious that the check can also be performed so that at the receiving end CRC is calculated from the received data 301 and it is re-XORed with the XORed data 308 so that the result is the authentication value Another authentication value can be derived somehow from the received data 301 As a result these two authentication values are compared 305 and if the comparison 305 equals, the data has been transmitted without any changes. If the result of the comparison is unequal the data received can be erased. A third possibility to check the validity of data is that the receiver derives an authentication value 202 and an error check value 303 from the received data 301 and XORs them. The result of this XORing is compared to the XORed data value 308 which is received. If the comparison equals the received data is valid, if not the data has been corrupted in the transmission path.

The input for the authentication value 202; 302 can preferably be a packet number or a secret key. At both ends it is used the same, advantageously secret, algorithm for calculating the authentication value 202; 302. As a result, the authentication value 202; 302 can for example be a CRC of the original data 201, which is encrypted with the secret key of the sender. To a man skilled in the art it is obvious that most preferably the authentication value 202; 302 is derived from such an input that is dependent on the data which is to be transmitted. One possible input for the authentication value 202; 302 is the direction (uplink or downlink) of transferred data packet

It is obvious that the data field can also be encrypted so that nobody not justified is capable to read the message. The methods shown previously can be used to perform this encryption.

One possible application of this invention is to use it in all solutions where the so called packet data transmission is used. As an example, we consider a situation

where a mobile station 101 is communicating with another mobile station 101 through the GPRS network. The mobile station 101 is arranged to secure the data to be transmitted so that nobody not justified is able to change the data. When the data is ready to be sent, the CRC 205 is derived from the digital data 201 in the transmitter block of the mobile station 101. As well the authentication value 202 is derived from the digital data 201 in the transmitter block. The CRC 205 and the authentication value 202 are combined together with a logical function 203. In the transmitter block of the mobile station 101 the original digital data 201 and the combination of the CRC 205 and authentication value 202 are arranged to the same data packet which data packet is sent

The data packet is transmitted for instance through the GPRS network to another mobile station 101. The receiver block of the mobile station 101 receives the data packet, or more precisely, the combination of blocks 301 and 308, and derives the authentication value 302 in the same way as at the transmitter block. This derived authentication value 302 is combined with the XORed data field 308 with the same logical operation 203, advantageously with XOR function, as in the transmitter block. The result of this combination is according to this preferred embodiment of the invention the CRC value 304. The receiver block derives another CRC 303 from the original data for checking, if the data is from the original sender. The check may be done by comparing 305 these two CRC values 303; 304. If the comparison 305 shows that the data is valid 306, the receiver block of the mobile station 101 passes the data onto the other blocks of the mobile station 101 so that the user of the mobile station 101 is able to find out the content of the data. If the comparison 305 fails, it shows that an unauthorized person has changed the data or the data has been corrupted during the transmission, the data can be erased 307 in the receiver block of the mobile station 101. Alternatively the data can be shown to the user of the mobile station 101 with the notification that the data has changed in the transmission path. To a man skilled in art it is obvious that the data transmitted between the user of the transmitting mobile station 101 and the user of the receiving mobile station 101 can be any type of data which is possible to transmit through a packet data network. Further, to a man skilled in the art it is obvious that the logical function shown previously may be implemented by using the logic gates in hardware. As well, the same can be achieved with software

Figure 4 shows a block diagram of a digital mobile communication means according to an advantageous embodiment of the invention. The mobile communication means comprises a microphone 401, keyboard 407, display 406, earpiece 414, antenna

duplexer or switch 408, antenna 409 and a control unit 405, which all are typical components of conventional mobile communication means. Further, the mobile communication means contains typical transmission and receiver blocks 404, 411. Transmission block 404 comprises functionality necessary for speech and channel coding, encryption, and modulation, and the necessary RF circuitry for amplification of the signal for transmission. Receiver block 411 comprises the necessary amplifier circuits and functionality necessary for demodulating and decryption of the signal, and removing channel and speech coding. The signal produced by the microphone 401 is amplified in the amplifier stage 402 and converted to digital form in the A/D converter 403, whereafter the the signal is taken to the transmitter block 404. The transmitter block encodes the digital signal and produces the modulated and amplified RF-signal, whereafter the RF signal is taken to the antenna 409 via the duplexer or switch 408 The receiver block 411 demodulates the received signal and removes the encryption and channel coding The resulting speech signal is converted to analog form in the D/A converter 412, the output signal of which is amplified in the amplifier stage 413, whereafter the amplified signal is taken to the earpiece 414 The control unit 405 controls the functions of the mobile communication means, reads the commands given by the user via the keypad 407 and displays messages to the user via the display 407. Further, in this preferred embodiment the transmitter block 404 comprises first means 416 for deriving an authentication value from the data to be transmitted, second means 417 for deriving an error check value from the data to be transmitted and third means 418 for combining said authentication value and said error check value with a logical function for producing a first reference value. Correspondingly, in this preferred embodiment the receiver block 411 also comprises first means 420 for deriving a first reference value from the received data, second means 421 for calculating a second error check value from the received data, third means 422 for calculating a second reference value at least partly based on a first and a second value from the set of said second error check value, a second authentication value and said first reference value, and fourth means 423 for comparing said second reference value with a third value from the set of said second error check value, said second authentication value and said first reference value The means mentioned can be any kind of arrangements which are capable to perform the operations described. For example the means can be computer programs, which are used by a microprocessor 415; 419 in a transmitter 404 and a receiver block 411 in a mobile station for performing the operations described.

The present invention is not limited to the embodiment of Fig. 4, which is presented as an example only. For example, the invention can as well be applied to an analog communication means.

The previously described data check can also be arranged so that the check is carried out in a network element. For example the GPRS network comprises a SGSN 108 which is communicating with the mobile station 101 through a logical link called LLC. LLC has a CRC function (ETSI GSM 03.60). According to one preferred embodiment of the invention the authentication value has been added to the CRC field to provide a per packet authentication. The benefit is that the network operator can be sure that the packet is originating from the valid user. This method can in certain cases (traffic is encrypted by the user, browsing public web sites) avoid the use of ciphering. Additionally, with this arrangement the network operator is capable of performing the billing according to the use of the network. To a man skilled in the art it is obvious that the SGSN 108 comprises the corresponding means 415; 416; 417; 418; 419; 420; 421; 422; 423 for checking the data as the receiver block 404 and the transmitter block 411. The network element mentioned can be any other network element than the SGSN 108. To a man skilled in the art it is obvious that the network element can in an advantageous embodiment of the invention comprise the means 415; 416; 417; 418; 419; 420; 421; 422; 423 described previously. The operations of the means can also be performed with any other possible way which is suitable for telecommunications.

For example the same operations can be performed in a transmitter block and in a receiver block of a base station.

The method shown can also be applied to file management and ciphering in computer systems. For example the operating system can check if the valid administrator has made the changes to the settings of the operating system by comparing the user-specific values which can be derived from the file the user has changed. If the settings file has been changed by any other person but the valid administrator the changes will be cancelled.

The packet data network may be any kind of network which is capable to transmit data as a data packets. In addition to GPRS network in GSM system or UMTS system the network can be for example an Internet Protocol network.

A digital signature created with the previously described public and secret key method can also be used as the authentication value in an advantageous embodiment

of the invention. The CRC value can be any other error check value which can be applied to the arrangements previously described.

To a man skilled in the art it is obvious that the original data 201 in the data packets can be encrypted so that it is not possible for persons not justified to find out the content of the message. One possible solution to achieve this is to use the public and secret key method for encrypting the original message before the previously described operation.

To a man skilled in the art it is obvious that the mobile station 101 mentioned can be understood as an any kind of station which is capable of transmitting data in data packets The station can be for example a computer device or any other kind of station which uses a wireless data transmission

As well it is obvious to a man skilled in the art that the term packet in this context can be understood as any kind of element, like a frame or a cell (in ATM), in which data is transferred.

Claims

1. A method for checking of data, **characterized** in that

- a first reference value is calculated at least partly based on a first error check value calculated from the data and a first authentication value (202)

2. A method according to claim 1, **characterized** in that when checking the data

- a second error check value is calculated from the data,

- a second reference value is calculated at least partly based on a first and a second value from the set of said second error check value, a second authentication value and said first reference value,

- said second reference value is compared with a third value from the set of said second error check value, said second authentication value and said first reference value

3 A method according to claim 1, **characterized** in that the data is in the form of packets to be sent from a transmitter to a receiver and said first reference value is added to the packet to be sent.

4. A method according to claim 3, **characterized** in that the data is to be sent in a cellular system.

5. A method according to claim 1, **characterized** in that said calculation is performed with the exclusive-OR function.

6 A method according to claim 2, **characterized** in that said first and second authentication values (202; 302) are derived at least partly based on a secret key.

7. A method according to claim 3, **characterized** in that said first and second authentication values (202; 302) are derived at least partly based on a packet number.

8. A method according to claim 3, **characterized** in that said first and second authentication values (202; 302) are derived at least partly based on the direction of the packet to be transmitted

9. A method according to claim 2, **characterized** in that said first and second error check values are CRC values (205; 303; 304).

10 A method according to claim 2, **characterized** in that said first and second authentication values are calculated at least partly based on the data.

11. A transmitter, **characterized** in that the transmitter comprises

- means for deriving an authentication value (202) from the data to be transmitted (201),

- means for deriving an error check value from the data to be transmitted (201) and

- means for combining said authentication value (202) and said error check value with a logical function for producing a first reference value.

12 A transmitter according to claim 9, **characterized** in that said logical function is exclusive-OR (203).

13. A receiver for receiving data having means for checking received data, **characterized** in that the receiver comprises

- means for deriving a first reference value from the received data,

- means for calculating a second error check value from the received data,

- means for calculating a second reference value at least partly based on a first and a second value from the set of said second error check value, a second authentication value and said first reference value, and

- means for comparing said second reference value with a third value from the set of said second error check value, said second authentication value and said first reference value.

14. A receiver according to claim 12, **characterized** in that the receiver is arranged to carry out the logical function exclusive-OR (203)

15. A station, comprising a transmitter and a receiver, **characterized** in that the transmitter comprises

- means for deriving an authentication value (202) from the data to be transmitted (201),

- means for deriving an error check value from the data to be transmitted (201) and

- means for combining said authentication value (202) and said error check value with a logical function for producing a first reference value

and

the receiver comprises

- means for deriving a first reference value from the received data,

- means for calculating a second error check value from the received data,

- means for calculating a second reference value at least partly based on a first and a second value from the set of said second error check value, a second authentication value and said first reference value, and

- means for comparing said second reference value with a third value from the set of said second error check value, said second authentication value and said first reference value.

16. A station according to claim 14, **characterized** in that the mobile station (101) is arranged to carry out the logical function exclusive-OR (203).

17. A station according to claims 14 or 15, **characterized** in that the station is a mobile station (101).

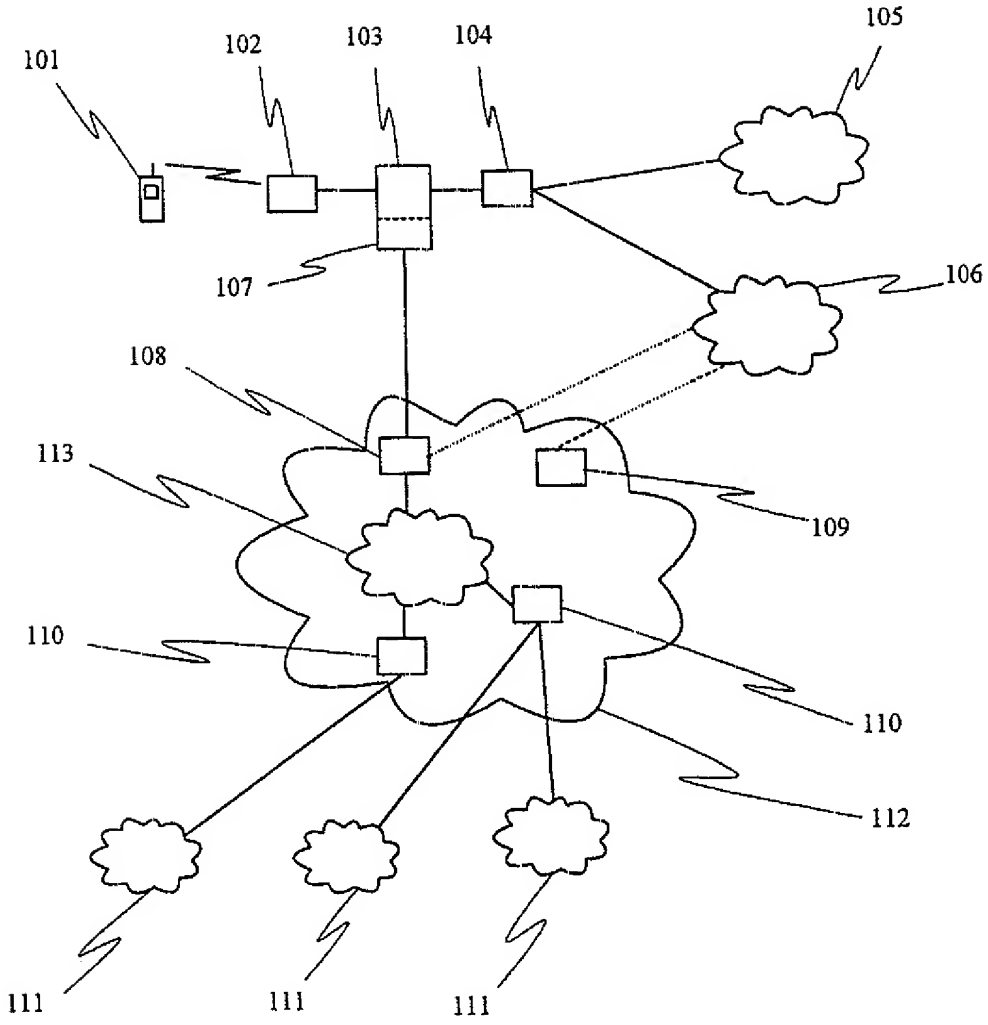


Fig. 1

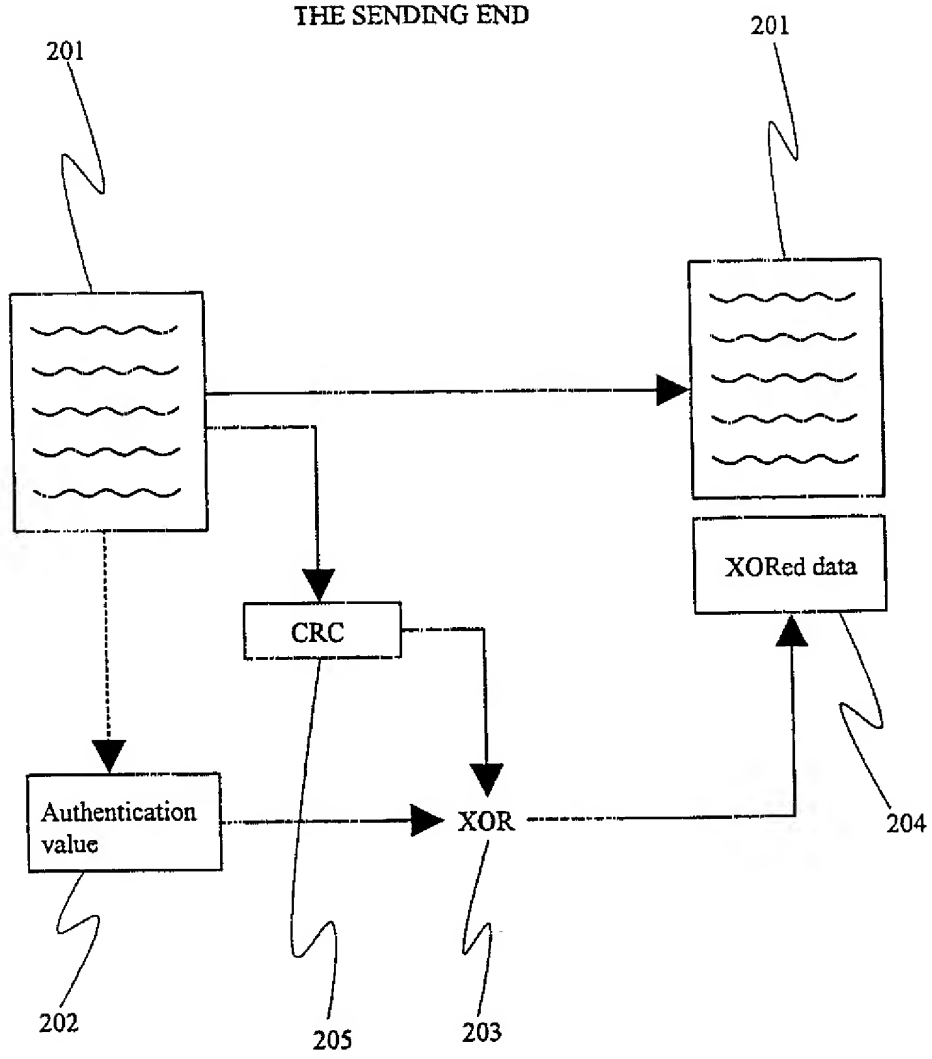

THE SENDING END
201
201
XORed data
CRC
Authentication value
XOR
204
202
205
203

Fig. 2

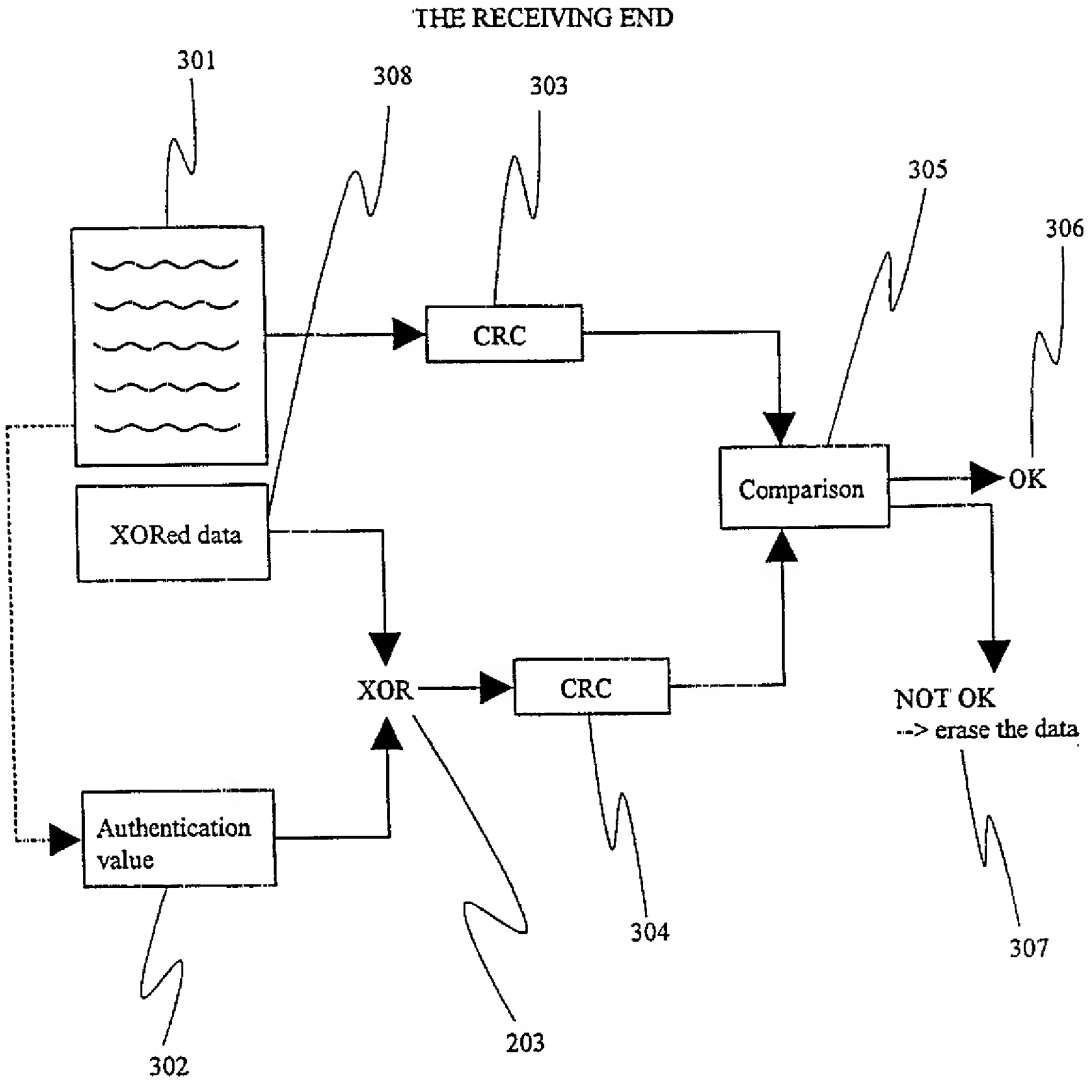

THE RECEIVING END
301
308
303
305
306
CRC
Comparison
OK
XORed data
XOR
CRC
NOT OK
--> erase the data
Authentication value
304
307
302
203

Fig. 3

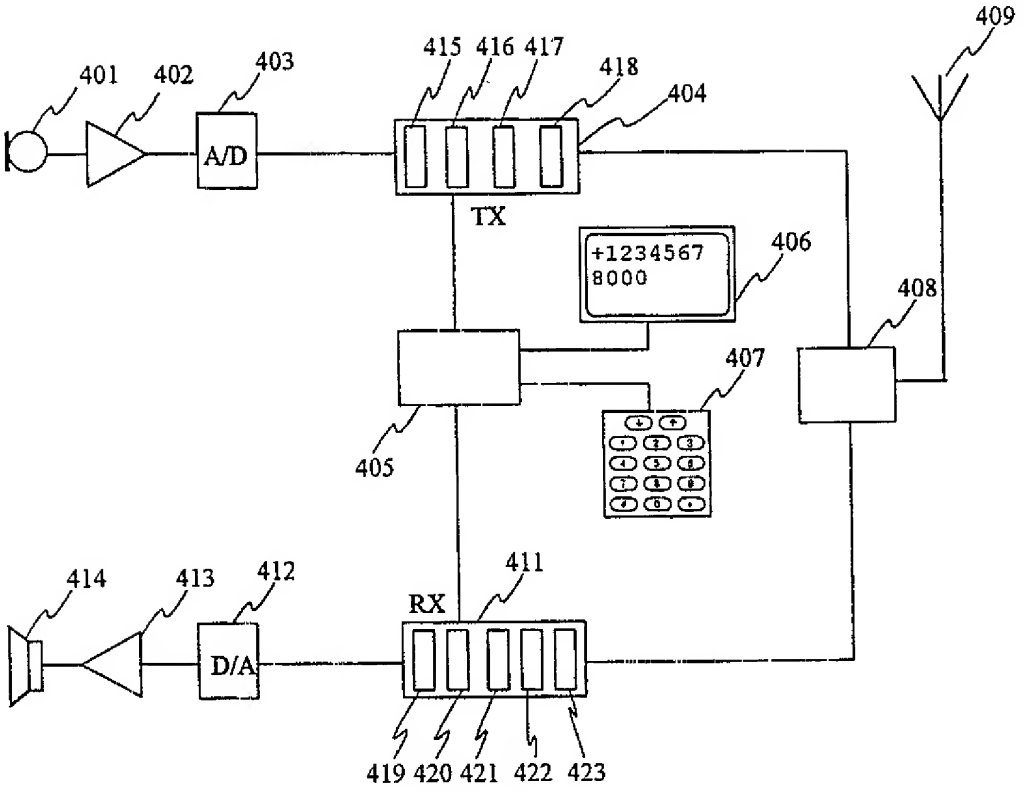

409
401
402
403
415
416
417
418
404
A/D
TX
+1234567
8000
406
408
407
405
414
413
412
411
RX
D/A
419
420
421
422
423

Fig. 4